UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

IN RE: PRACTICEFIRST DATA BREACH LITIGATION

1:21-CV-00790(JLS/MJR)
REPORT AND RECOMMENDATION

INTRODUCTION

This case has been referred to the undersigned by the Honorable John L. Sinatra, Jr., pursuant to Section 636(b)(1) of Title 28 of the United States Code, for all pretrial matters and for hearing and reporting on dispositive motions for consideration by the District Court. (Dkt. No. 17) Before the Court is defendants' motion to dismiss the complaint pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, based on lack of subject matter jurisdiction and failure to state a claim on which relief can be granted. (Dkt. No. 23) For the following reasons, it is recommended that defendants' motion to dismiss the complaint for lack of subject matter jurisdiction pursuant to Rule 12(b)(1) be granted.

BACKGROUND

On July 9, 2021, plaintiffs Peter Tassmer and Karen Cannon filed a complaint, on behalf of themselves and a class of others similarly situated, based on a December 30, 2020 data breach of defendants Professional Business System d/b/a Practicefirst Medical Management Solutions and PBS Medcode Corp.'s ("Practicefirst" or "defendants") computer system, which involved the unauthorized disclosure of personal and confidential

information belonging to plaintiffs and other individuals. (Dkt. No. 1) A consolidated class action complaint was filed on October 21, 2021.[1] (Dkt. 22)

Defendants moved to dismiss the consolidated class action complaint on November 22, 2021. (Dkt. No. 23) Plaintiffs filed a response on December 19, 2021 (Dkt. No. 25) and defendants replied on January 4, 2022 (Dkt. No. 27). The Court heard oral argument on January 13, 2022.

COMPLAINT ALLEGATIONS

Practicefirst is a medical management company hired by medical providers to conduct billing, credentialing, coding, compliance, chart auditing, bookkeeping, tax preparation, and other similar services. (Dkt. No. 22, ¶2) Practicefirst's clients include 75 physician groups or medical practices across the country. (*Id.* at ¶12) Practicefirst maintains, on its computer system, the private health information ("PHI") and personally identifiable information ("PII") of individuals who are patients of its clients. (*Id.*) Plaintiffs Peter Tassmer, Karen Cannon, Paul Commisso and Glenda Johnson are all patients of medical providers who contracted with Practicefirst, and whose PHI and PII was stored on Practicefirst's computer system. (*Id.* at ¶¶8-12)

The complaint alleges that on December 30, 2020, Practicefirst discovered that an unauthorized third party had "accessed its computer system and copied (exfiltrated) files," which included the confidential or private data of over 1.2 million patients or employees

[1] The consolidated complaint was filed pursuant to a Stipulation and Order, entered on September 21, 2021 by the District Court, which consolidated, for pre-trial purposes, the matters of *Tassmer et al. v. Professional Business Services d/b/a PracticeFirst Medical Management Solutions and PBS Medcode Corp.*, No. 1:21-cv-00970, filed July 9, 2021, and *Commisso et al. v. Professional Business Services*, No. 1-21-cv-00937, filed August 17, 2021, as well as any subsequently filed related actions, pursuant to Federal Rule of Civil Procedure 42(a). (Dkt. No. 15)

(the "data breach"). (*Id.* at ¶4, ¶18) Practicefirst was then subjected to a ransomware attack in connection with the data breach. (*Id.* at ¶40-¶46) The complaint describes a ransomware attack as "a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the owner pays a fee to the perpetrator." (*Id.* at ¶40) Practicefirst hired a forensic investigation firm to determine the exact nature and scope of the data breach. (*Id.* at ¶19) It was determined that while the information accessed during the data breach varied by individual, the categories of patient and employee information copied by the third party included names; addresses; email addresses; dates of birth; driver's license numbers; social security numbers; medical diagnosis; treatment information; patient identification numbers; employee usernames and passwords; bank account information; and credit and/or debit card information. (*Id.* at ¶6, ¶20) The investigation also revealed that 1,210,688 individuals were impacted by the breach. (*Id.* at ¶20)

Plaintiffs were notified of the data breach in June and July of 2021.[2] (*Id.* at ¶27, ¶30, ¶33, ¶36) According to the complaint, plaintiffs were informed that their PII/PHI had been accessed and "copied by an unauthorized actor before it was permanently deleted."[3] (*Id.* at ¶21) The notification letters instructed plaintiffs to, among other things, "regularly

---

[2] Plaintiffs Tassmer and Cannon received notice of the data breach on July 3, 2021. (*Id.* at ¶27, ¶30) Plaintiffs Commisso and Johnson received notice on June 30, 2021. (*Id.* at ¶33, ¶36) During oral argument, defense counsel explained that while the data breach was discovered on December 30, 2020, it took Practicefirst additional time to determine the scope of the breach and the identities of all the patients and employees affected. Defense counsel indicated that individuals were then notified, on a rolling basis, when it was determined that their specific data had been involved in the breach.

[3] The complaint states that even if the unauthorized party later claimed they deleted the exfiltrated PII/PHI, computer experts have definitively stated that "Proof of deletion is not a thing." (*Id.* at ¶22) Thus, it is alleged that even though the unauthorized party or hackers apparently represented to defendants that the exfiltrated data was deleted after the "ransom" or fee was paid, there is no way to know, for certain, that the hackers did not retain a copy of the confidential data that was exfiltrated during the breach. (*Id.*)

review account statements and report any suspicious activity to financial institutions." (*Id.* at ¶27, ¶30, ¶33, ¶36) The letters also provided plaintiffs an option to enroll in credit monitoring and identity theft recovery services. (*Id.*) During oral argument, defense counsel represented that Practicefirst offered to pay the costs for plaintiffs, and any others affected by the data breach, to enroll in a credit monitoring service.

Plaintiffs Tassmer, Cannon, Commisso and Johnson all allege that after receiving notification of the data breach, they spent time reviewing their account statements and credit reports for any indication of actual or attempted identity theft, and that this was valuable time which could have been spent on other activities. (*Id.* at ¶28, ¶31, ¶34) Plaintiffs Commisso and Johnson further allege that their efforts included "time spent on the telephone and sorting through unsolicited spam, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring sensitive accounts." (*Id.* at ¶34, ¶37) Plaintiffs allege that "actual" injuries experienced from having their PII/PHI comprised include: "(a) damage to and diminution in the value of [their] PII/PHI; (b) violation of [their] privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft, and financial and medical fraud." (*Id.* at ¶29, ¶32, ¶35, ¶38) Plaintiffs anticipate spending "additional time and money on an ongoing basis to try and mitigate and address the harms caused by the Data Breach." (*Id.* at ¶25, ¶39, ¶88)

Plaintiffs bring the instant lawsuit as a class action and seek to represent a proposed nationwide class defined as "All persons residing in the United States whose PII/PHI was compromised in the Data Breach that Practicefirst announced on or about June 30, 2021." (*Id.* at ¶¶90-101) The causes of action asserted in the complaint, on

behalf of plaintiffs and the proposed class, are: (1) breach of the contract between defendant and the medical providers, to which plaintiffs allege they were intended third-party beneficiaries; (2) negligence based on defendants' breach of their duty to protect class members' PHI/PPI; and (3) declaratory and injunctive relief.[4] (*Id.* at ¶102-140)

DISCUSSION

Federal Rule of Civil Procedure 12(b)(1) and Subject Matter Jurisdiction

To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(1), a plaintiff must establish subject matter jurisdiction. *See Makarova v. United States*, 201 F.3d 110, 113 (2d Cir. 2000). In resolving a motion to dismiss for lack of subject matter jurisdiction, a court is required to accept as true the factual allegations contained in the complaint. *See Morrison v. Nat'l Australia Bank Ltd.*, 547 F.3d 167, 170 (2d Cir. 2008). "The plaintiff bears the burden of proving subject matter jurisdiction by a preponderance of the evidence." *Aurecchione v. Schoolman Transp. Sys., Inc.*, 426 F.3d 635, 638 (2d Cir. 2005).

"Standing is 'the threshold question in every federal case' and implicates the Court's subject matter jurisdiction." *Cohan v. Motady*, 751 F. Supp. 2d 436, 439 (E.D.N.Y. 2010); *quoting Ross v. Bank of Am., N.A. (USA)*, 524 F.3d 217, 222 (2d Cir. 2008). To establish standing under Article III of the Constitution, a plaintiff must show: "(1) an injury-in-fact; (2) a causal connection between that injury and the conduct at issue; and (3) a likelihood that the injury will be redressed by a favorable decision." *Maddox v. Bank of New York Mellon Trust Co.*, 19-CV-1774, 2021 U.S. App. LEXIS 34056 (2d Cir. Nov. 17,

[4] The injunctive relief requested by plaintiffs includes requiring defendants to (1) strengthen their security systems and data monitoring procedure; (2) submit future audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to class members. (*Id.* at ¶125, ¶133)

2021) (internal quotations omitted). To demonstrate injury-in-fact, a plaintiff must show "the invasion of a (1) legally protected interest that is (2) concrete and particularized and (3) *actual or imminent*, not conjectural or hypothetical." *Id.* at *3 (emphasis added). In the class action context, plaintiffs "must allege and show that they personally have been injured[.]" *Warth v. Seldin*, 422 U.S. 490, 503 (1975). Thus, "if none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974).

Here, defendants argue that plaintiffs lack Article III standing to sue because they fail to allege an injury-in-fact. Specifically, defendants contend that plaintiffs have not shown that they experienced concrete harm arising from the data breach or a threat of future harm that is actual or imminent. For the following reasons, the Court agrees and recommends dismissal of the consolidated class action complaint on this basis.

Recent Supreme Court and Second Circuit Cases Addressing Standing

In *Clapper v. Amnesty International*, the Supreme Court made clear that "allegations of possible future injury" or even an "objectively reasonable likelihood" of future injury are insufficient to confer standing. 568 U.S. 398, 408-409 (2013). Rather, a future injury constitutes an Article III injury-in-fact only "if the threatened injury is certainly impending." *Id.* (plaintiffs may not rely on "a highly attenuated chain or possibilities" or a "speculative chain of events" to establish standing).

In the recent decision of *TransUnion v. Ramirez*, the Supreme Court further narrowed Article III standing requirements by holding that a plaintiff cannot establish an injury-in-fact, for purposes of standing, by relying entirely on a risk of future harm.

TransUnion v. Ramirez, 141 S. Ct. 2190 (2021). The Supreme Court instructed that, "in a suit for damages the mere risk of future harm, standing alone, cannot qualify as concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm." *Id.* at 2210-11. Stated simply, "[n]o concrete harm, no standing." *Id.* at 2200.[5] The Supreme Court went on to explain that whether a harm qualifies as "concrete" hinges on "whether the alleged injury to the plaintiff has a close relationship to harm traditionally recognized as providing the basis for a lawsuit in American courts." *Id.* at 2200. The allegations in *TransUnion* involved inaccurate credit reports which wrongly identified plaintiffs as potential terrorists or high-risk criminals. *Id.* at 2201-03. Applying these Article III standing principles to the facts at hand, the *TransUnion* Court ruled that plaintiffs whose inaccurate credit reports were actually sent to third parties had standing to sue the credit agency, since they suffered a concrete harm with a "close relationship" to the reputational tort of defamation. *Id.* at 2207. However, plaintiffs whose inaccurate credit reports were not sent to any third parties did not have standing to sue, since, by contrast, they suffered only a "mere procedural violation, divorced from any concrete harm." *Id.* at 2213. The *TransUnion* Court rejected the argument that individuals whose credit reports had not been released could proceed in the lawsuit by showing a risk that the reports might be disseminated in the future. *Id.* at 2211. Instead, the Supreme Court

---

[5] The *TransUnion* Court distinguished its decision in *Clapper v. Amnesty Int'l* in that *Clapper* involved a suit for injunctive relief. *Id.* at 2210. The *TransUnion* Court noted that "a person exposed to risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *Id.* However, a different showing is required in a suit for damages since "a plaintiff's standing to seek injunctive relief does not necessarily mean that the plaintiff has standing to seek retrospective damages." *Id.* Here, plaintiffs seek both damages and injunctive relief. For the reasons to be explained herein, plaintiffs have established neither the imminent risk of harm necessary to warrant injunctive relief nor have they shown the imminent risk of future harm combined with actual concrete harm needed to support a claim for damages.

qualified that this risk would need to have caused plaintiffs "some other injury" to furnish Article III standing.[6] *Id.*

Recently, in *Maddox v. BNY Mellon*, the Second Circuit applied the requirements of *TransUnion* and found that plaintiffs did not have standing to bring a class action lawsuit against a defendant bank for violations of New York's mortgage-satisfaction-recording statutes since plaintiffs suffered no concrete or particularized injury. 19-17774, 2021 U.S. App. LEXIS 34056 (2d Cir. Nov. 7, 2021). Plaintiffs argued that they had sufficiently alleged a risk of future harm because the bank's failure to timely file documents showing that plaintiffs satisfied their mortgage debt could have clouded title to plaintiffs' property or shown a debt to prospective creditors that plaintiffs did not owe, which may have impacted their credit score or ability to get a loan. *Id.* The Second Circuit, relying on *TransUnion*, rejected this argument.

> True, [plaintiffs] may have suffered a nebulous risk of future harm during the period of delayed recordation—i.e., a risk that someone (a creditor, in all likelihood), might access the record and act upon it—but that risk, which was not alleged to have materialized, cannot form the basis of Article III standing.

Id. at *15-16. In addition, one plaintiff submitted an affidavit indicating that the defendant bank's failure to record the mortgage satisfaction caused her great stress, mental anguish, and anxiety. *Id.* at *17. She also claimed to have spent substantial time determining the status of the recording and engaging legal counsel to assist in having the mortgage satisfaction recorded. The Second Circuit acknowledged that these purported harms were the sort that *TransUnion* contemplated *may* form the basis of Article III

[6] The *TransUnion* Court also noted that, apart from the fundamental problem that plaintiff's standing was based only on a risk of future harm, plaintiffs also failed to show a sufficient risk that their credit reports would be disseminated to third parties, and thus their allegation of future harm was also "*too speculative* to support Article III standing." *Id.* at 2211-12 (emphasis added).

standing. *Id.* at *15; *accord TransUnion*, 141 S. Ct. at 2211 n.7 ("A plaintiff's knowledge that he or she is exposed to a risk of future physical, monetary or reputational harm could cause its own current emotional or psychological harm.") However, the *Maddox* Court determined that the plaintiff made only a "perfunctory allegation" of emotional distress that was "wholly incommensurate with the stimulant" and therefore insufficient to grant standing. *Id.* at *17-18.

In sum, *Clapper*, *TransUnion,* and *Maddox* instruct that to establish Article III standing in a suit for damages, a plaintiff must allege *both* a risk of future harm that is "actual and imminent" or "certainly impending" *as well as* a separate, concrete harm that was caused by exposure to the imminent risk and is proportional to the actual likelihood of the future harm occurring. To that end, the Supreme Court has made clear that allegations of a concrete harm that are tied to speculative or possible future injury are insufficient because plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 416.

Here, plaintiffs contend that they have standing because they experienced a risk of future harm, *i.e.*, an ongoing and increased risk that they will be victims of identity theft or other types of fraud because of the data breach. Plaintiffs also allege actual or concrete harm in the form of their mitigation efforts, *i.e.,* the time, energy, and resources they spent researching the data breach and ensuring the security of their accounts. According to the complaint, this includes time spent on the telephone; time spent "sorting through unsolicited spam"; the investigation of credit monitoring services; researching the data

breach; and having to closely monitor their accounts and credit reports. For the following reasons, the Court rejects plaintiffs' theory of standing.

Plaintiffs have not alleged an imminent or certainly impending risk of future harm.

In *McMorris v. Carlos Lopez and Associates, LLC,* the Second Circuit identified three factors a district court should consider in determining whether an increased risk of identity theft following disclosure of personal data is sufficiently "concrete, particularized and imminent" to confer standing. 995 F.3d 295, 300 (2d Cir. 2021). These factors are: (1) whether the plaintiff's data has been exposed as part of a targeted attempt to obtain the data; (2) whether any portion of the data has already been misused, even if plaintiffs themselves did not experience any fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud. *Id.* at 300-01. Plaintiffs contend that the *McMorris* factors, applied to the allegations presented here, weigh in favor of standing. Defendants counter that because *McMorris* was decided prior to the Supreme Court's decision in *TransUnion*, its three-factor test is no longer applicable to plaintiffs' claims for damages. The Court finds, however, that it need not specifically determine whether *McMorris* applies in the same manner as it did before the *TransUnion* decision. Below, the Court has applied the three-factor *McMorris* test to the allegations here, as advocated by plaintiffs, and still finds an insufficient showing of imminent or certainly impending harm to confer standing.[7]

[7] In *McMorris*, the Second Circuit seemed to hold that a plaintiff could establish standing based on an increased risk of identity theft alone if the risk of future injury is imminent. As just discussed, *TransUnion* has abrogated this holding in suits for damages by requiring both an imminent risk of future harm *and* a concrete injury related to the risk. However, the Court finds that *McMorris'* three-factor test is still instructive for determining whether the risk of injury is imminent, which remains part of the requirement for standing in suits for both damages and injunctive relief, pursuant to *TransUnion* and *Clapper*.

With respect to the first factor, the complaint fails to plausibly allege that the December 30, 2020 data breach was a targeted attempt to expose or copy plaintiffs' confidential data for purposes of identity theft or other similar-type fraud. The complaint states that plaintiffs' PPI and PHI, along with the PPI and PHI of over a million other individuals, was exfiltrated or copied by an unauthorized third party or hacker. It is then alleged that defendants experienced a ransomware attack related to the data breach. As described in the complaint, a ransomware attack involves the denial of access to information until the subject of the attack pays a fee or "ransom" to regain use of its data. Here, the complaint suggests that defendants' access to the information was ultimately reinstated, presumably after payment of a fee. Indeed, the primary purpose of a ransomware attack is the exchange of money for access to data, not identity theft. Plaintiffs seem to concede this fact. However, plaintiffs maintain that because their PPI and PHI was exfiltrated or copied from defendants' system as part of the ransomware attack, the hacker must intend to use the data, in the future, for identity theft or fraud. This suggestion is both speculative and belied by the complaint, which fails to allege that *any* of the over 1.2 million people affected by the data breach have experienced attempted or actual identity theft, or a similar type of fraud or attempted fraud, in over a year following the ransomware attack. Thus, plaintiffs do not plausibly allege that this data breach was the type of cyber-attack targeted to obtain confidential information for purposes of identity theft, as opposed to garden-variety ransomware attack. Moreover, the general allegations in the complaint that individuals whose confidential information has been exposed during a data breach are more likely to experience identity theft in the future are insufficient and conclusory, and do not raise plaintiffs' claim that they are at imminent risk of future harm

above a speculative level. *See Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524 (D. Mass. 2016) (plaintiff whose personal information was disclosed to hackers through phishing email failed to allege a "certainly impending" or "substantial risk" of injury sufficient to establish Article III standing because the complaint did not allege a clear intent to use the data to engage in identity theft or fraud, and "general allegations—that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft, do not alter this conclusion.").

Indeed, the Court finds this scenario analogous to *Graham v. Universal Health Serv.*, where the Eastern District of Pennsylvania Court refused to confer standing to plaintiffs based on their alleged increased risk of identity theft following exposure of their confidential information in a ransomware attack, since it was "purely speculative" that hackers intended to use plaintiffs' data for any future criminal acts beyond the initial ransomware attack. 20-5375, 2021 U.S. Dist. LEXIS 93075 (E.D. Pa. May 17, 2021) (noting that the "target of a ransomware attack is the holder of the confidential data; the misappropriation of the data, whether by theft or merely limitation on access to it, is generally the means to an end: extorting payment"). *See also Quintero v. Metro Santurce, Inc.*, 20-01075, 2021 U.S. Dist. LEXIS 237071 (D. PR Dec. 9, 2021) (motion to dismiss granted for lack of Article III standing where class action complaint alleged only a "garden-variety ransomware attack" and "there [were] no sufficiently pleaded allegations of a motive to seal the PII for identity theft or fraud."); *Travis v. Assured Imaging LLC*, 20-00390, 2021 U.S. Dist. LEXIS 89129 (D. AZ May 10, 2021) (motion to dismiss class action complaint based on data breach granted for lack of standing in part because allegations of a ransomware attack did not indicate that the data was taken in a "manner that

suggests it will be misused."). Likewise, because the complaint here does not allege facts showing a targeted attempt or clear intent to obtain plaintiffs' confidential information for its future misuse, the first *McMorris* factor does not weigh in favor of standing.

As for the second *McMorris* factor, plaintiffs fail to allege that any of the compromised data has been misused.[8] Indeed, over a year has passed since the data breach and there is no indication that plaintiffs, or any of the other potential class members for that matter, have had their identities stolen. In fact, the complaint is devoid of allegations that class members have experienced any type of fraud because of the breach, or even that attempts have been made to use their personal information for nefarious purposes. In *Fero v. Excellus Health Plan, Inc.* it was determined that plaintiffs' allegations of an increased risk of harm following a data breach, unaccompanied by any concrete misuse of their personal information, did not constitute actual or imminent

[8] During oral argument, plaintiff's counsel attempted to argue that the complaint does, in fact, allege misuse of data because it alleges that two of the named plaintiffs received "unsolicited spam." The Court rejects this argument. First, counsel's reading of the complaint is incorrect. The complaint alleges that plaintiffs made "reasonable efforts to mitigate further impact of the data breach" and that this "included time spent on the telephone and sorting through unsolicited spam." (Dkt. No. 22) Nowhere in the complaint does it allege, with any plausible details or specificity, that plaintiffs received "unsolicited spam", or an increase in spam, *because of* the December 30, 2020 data breach. *See Cooper v. Bonobos*, 21-CV-854, 2022 U.S. Dist. LEXIS 9469 (SDNY Jan. 6, 2022) (no injury in fact where plaintiff did not demonstrate that spam texts, calls, and email were "fairly traceable" to defendant's data breach.). Moreover, even if plaintiffs had shown that they received an increase in spam because of this data breach, the Court would still find these allegations insufficient to allege injury in fact. *See Legg v. Leaders Life Ins. Co.*, 21-655, 2021 U.S. Dist. LEXIS 232833 (W.D. Okla. Oct. 1, 2021) (the receipt of phishing emails, while perhaps "consistent with" data misuse, does not "plausibly suggest" that any actual misuse of plaintiff's personal identifying information has occurred); *Travis*, 2021 U.S. Dist. LEXIS 89129, *19 ("a dramatic increase in targeted spam phone calls after [a] ransomware attack" did not constitute an injury for purposes of standing); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605 (SDNY Mar. 12, 2009) ("The receipt of spam by itself...does not constitute a specific injury entitling [plaintiff] to compensable relief."); *Gordon v. Virtumundo, Inc.*, 06-0204, 2007 U.S. Dist. LEXIS 35544 (W.D. Wash. May 15, 2007) (plaintiff lacked standing because the harm suffered "must rise beyond the level typically experienced by consumers – i.e., beyond the annoyance of spam.").

injuries, since "the alleged injuries rely on a chain of possibilities about the actions of independent actors." 236 F. Supp. 3d 735 (WDNY Feb. 22, 2017). Likewise here, plaintiffs have alleged only a speculative or possible risk of future harm, rather than an imminent or certainly impending injury. *See also Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577 (EDNY 2015) (plaintiff failed to allege an injury that was "certainly impending" or based on a "substantial risk that the harm will occur" where nearly two years passed since the security breach, and no plaintiff has experienced fraudulent charges); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605 (SDNY 2009) ("[T]he release of potentially sensitive information alone, without evidence of misuse, is insufficient to cause damage to a plaintiff" and "the risk of some unidentified future harm is too speculative to constitute a compensable injury."). Thus, the second *McMorris* factor weighs against standing.[9]

Indeed, numerous circuit and district courts have declined to grant standing based on an imminent risk of future identity theft where plaintiffs, like plaintiffs here, were unable to show that either their data, or the data of other victims of a data breach or cyber-attack, was actually misused. The Court is in agreement with their reasoning and finds these cases to be analogous to the matter at hand. *See e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d Cir. 2011) (dismissing case at the pleadings stage and concluding that "[i]n

[9] The Court finds the cases predominately relied upon by plaintiffs to show imminent risk of harm to be distinguishable because in those cases, unlike the complaint here, plaintiffs had alleged misuse of the data of at least some proposed class members. For example, the complaint in *In re GE/CBPS Data Breach Litig* apparently included allegations that some proposed class members had experienced "fraudulent debit charges" and that their cards had been "canceled, suspended, or otherwise rendered unusable." 20 Civ. 2903, 2021 U.S. Dist. LEXIS 14602, *4 (SDNY Aug. 4, 2021). In *In re Blackbaud, Inc.*, thirty-one of the named plaintiffs asserted that they experienced actual identity theft or fraud as a result of the cyber-attack. 3:20-mn-02972, 2021 U.S. Dist. LEXIS 67954 (D.S.C. June 1, 2021). Likewise, in *McFarlane v. Altice USA, Inc.*, it was alleged that several plaintiffs experienced identity theft because of disclosure of their social security numbers. 20-CV-1297, 2021 WL 860584 (SDNY 2021).

data breach cases where no misuse is alleged…there has been no injury" and any damages that may occur are "entirely speculative and dependent on the skill and intent of the hacker."); *Alleruzzo v. SuperValu, Inc.*, 870 F.3d 763, 766 (8th Cir. 2017) (dismissing certain plaintiffs from case for lack of standing at pleadings stage because allegations that "illicit websites are selling their [credit card information] to counterfeiters and fraudsters" were speculative and failed to allege any injury); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021) (dismissal for lack of standing because conclusory allegations of a continuing risk of identity theft "without specific evidence of some misuse of class members' data does not establish a concrete injury."); *Beck v. McDonald*, 848 F.3d 262, 273-76 (4th Cir. 2017) ("mere theft" of plaintiff's data, without something more, required the consideration of the "attenuated chain of possibilities" rejected by *Clapper* [and] this theory of harm was simply 'too speculative' to constitute an injury in fact'") (internal citations omitted); *Khan*, 188 F. Supp. 3d at 531 ("In the absence of specific incidents of the use of stolen data for identity fraud purposes, district courts have generally found that the increased risk of identity theft does not confer standing."); *Legg v. Leaders Life Ins. Co.*, 21-655, 2021 U.S. Dist. LEXIS 232833 (W.D. Okla. Oct. 1, 2021) (dismissing a class action complaint involving a data breach for lack of standing where plaintiff's allegations, at best, "lead to a plausible inference that at some unknown time in the future, some of the putative class members may be the victim of identity theft or fraud [and] even accepting as true plaintiff's allegations about the nature of the breach, that it was an attack by cybercriminals – plaintiff only pleads facts showing that there is a non-imminent risk of possible future injury following the data breach.").

As for the final *McMorris* factor, the Court notes that the information disclosed in the data breach, which included social security numbers, was the sort of PII that might subject plaintiffs to an increased risk of identity theft or fraud. However, this factor alone does not establish an injury-in-fact, "in absence of any other facts suggesting that the PII was intentionally taken by an unauthorized third party or otherwise misused." *McMorris*, 995 F.3d at 303. "To hold otherwise would allow plaintiffs to string together a lengthy chain of possibilities resulting in injury." *Clapper*, 568 U.S. at 410. Thus, like the Second Circuit ultimately concluded in *McMorris*, the sensitive nature of plaintiffs' PPI and PHI that was exposed during the data breach here "does not, by itself, demonstrate that plaintiffs are at a substantial risk of future identity theft of fraud." *McMorris*, 995 F.3d at 303.

Plaintiffs have not alleged actual or concrete harm.

"Where plaintiffs have shown substantial risk of future identity theft or fraud, any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact." *McMorris*, 995 F.3d at 303. Conversely, "where plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury." *Id. See also Fero*, 236 F. Supp 3d at 753 ("This rule from *Clapper* has been applied in the data breach context, such that courts have concluded that mitigation efforts following a data breach do not confer standing where the alleged harm is not imminent.")

For the reasons just stated, plaintiffs have failed to allege an imminent risk of harm. Thus, while it may have been reasonable for plaintiffs to take some steps to mitigate the risk associated with the data breach, such as monitoring their accounts more closely or

enrolling in the free credit monitoring services offered by defendants, those actions cannot create a concrete injury where there is no imminent or substantial risk of harm. *See also Maddox*, 2021 U.S. App. LEXIS 34056, at *15-18 (emotional distress or actions taken to prevent a risk that were "wholly incommensurate with the stimulant" are not enough to establish standing); *Tsao*, 986 F.3d at 1344 (Plaintiff "cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft."); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (mitigation costs are insufficient to confer standing because there is no substantial risk of identity theft, and plaintiff's "assertion of wasted time and effort necessarily rose or fell alone with the Court's determination of whether there was substantial risk of harm."); *Reilly*, 664 F.3d at 38 ("costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury'.") (internal citations omitted).

The Court also finds that plaintiffs have failed to allege a concrete or actual injury based on a diminution in value of their PHI and PII as a result of the data breach. The complaint contains general and conclusory allegations that PII/PHI is a "valuable commodity" on the "cyber black-market" and that "many companies now offer consumers an opportunity to sell this information to advertisers and other third parties." However, plaintiffs do not allege that they attempted to sell their personal information and were forced to accept a decreased price, nor do they allege any details as to how their specific, personal information has been devalued because of the breach. *See Wallace v. Health Quest Sys.*, 20 CV 545, 2021 U.S. Dist. LEXIS 54557 (SDNY Mar. 22, 2012) (no injury where plaintiffs provided only speculative allegations regarding the value of their private

information on [the] black market and how their private information diminished in value); *Pena v. British Airways, PLC (UK)*, 18-CV-6278, 2020 WL 3989055 at *3 (EDNY Mar. 30, 2020) (finding no injury based on alleged diminution in value where plaintiff "had not alleged that he was offered or forewent any opportunity to profit from the sale of his personal information"); *Fero*, 236 F. Supp. 3d at 735 (mere allegation that data "commands a high price on the black market" is not sufficient to establish injury).

The Court further rejects any attempt by plaintiffs to establish standing based on a "violation of their privacy rights." The tort of public disclosure of private information is a common-law tort, pursuant to which a defendant who "gives publicly to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person and, and (b) is not of legitimate concern to the public." *See* 2021 U.S. App. LEXIS 32325, *Rest. (2d) of Torts* §652D (1977). First, the allegations here do not fit these elements. The complaint alleges that a massive amount of data was copied by a hacker and held hostage for payment of a fee. The complaint does not allege that Practicefirst directly disclosed plaintiffs' confidential information to the public at large. Indeed, the breach involved the PHI/PII of over 1.2 million people and there are no allegations in the complaint to indicate that plaintiffs' particular private information was ever specifically viewed by any one person, let alone that it was disclosed "publicly." The Court finds the circumstances here like *Ciccone v. Cavalry*, where an Eastern District of New York Court rejected a theory of standing based on public disclosure of private facts premised on the release of plaintiffs' debt-related information to a third-party vendor and its employees. 21-CV-2428, 2021 U.S. Dist. LEXIS 228037 (EDNY Nov. 29, 2021). The

Eastern District of New York Court logically reasoned that communication to a small group of people did not constitute public disclosure and emphasized that courts analyzing the tort of public disclosure of private information have required "publicly in the broad, general sense of the word 'public'." *Id.* at *10; *quoting Tureen v. Equifax, Inc.*, 571 F.2d 411, 418 (8th Cir. 1978) (noting that, in the context of an invasion of privacy claim publicly means "that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.").[10]

Moreover, even if plaintiffs could plead facts sufficient to allege the tort of public disclosure of private information, the Court would still find a lack of subject matter jurisdiction here. Indeed, this theory of standing has been rejected in the data breach context where, like in this case, plaintiffs have failed to demonstrate any concrete or particularized injury associated with the disclosure. *See Kahn*, 188 F. Supp. 3d at 533 (rejecting plaintiff's argument that the data breach caused a loss of privacy that constituted an injury-in-fact because no potential damages were identified arising from the loss and therefore plaintiff failed to allege a concrete and particularized injury); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962, n. 5 (Dist. Nev. 2015) (plaintiffs who failed

[10] In contrast, in *Bohnak v. Marsh & McLennan Cos.*, a Southern District of New York Court found that plaintiffs had standing to sue for alleged injuries arising from a data breach that compromised plaintiffs' PII, because the claim was analogous to the common-law tort of public disclosure of private information, and even though defendants did not willfully disclose and publicize plaintiffs' confidential information. 21 Civ. 6096, 2022 U.S. Dist. LEXIS 8256 (SDNY Jan. 17, 2022). The *Bohnak* decision is not binding precedent for this Court, and the Court declines to follow its reasoning here. Further, while the Court in *Bohnak* concluded that plaintiffs had standing, the Court still dismissed plaintiffs' claims for failure to plausibly allege damages. *16-19. To that end, the *Bohnak* Court reasoned that plaintiffs' allegations that they suffered a loss of time and money responding to an increased risk of identity theft were not cognizable damages because they were not proximately caused by the disclosure. *Id.*

to establish standing based on imminent risk of future harm caused by data breach could not establish standing on alternative theory of loss of privacy because "even if Plaintiffs adequately allege a loss of privacy, they have failed to show how that loss amounts to a concrete and particularized injury."); *Allison v. Aetna, Inc.*, 09-2560, 2010 U.S. Dist. LEXIS 22373 (E.D. Pa. Mar. 9, 2010) (no standing in data breach case, even where claim involved invasion of privacy); *Giordano v. Wachovia Sec., LLC*, 06-476, 2006 U.S. Dist. LEXIS 52266 (D. N.J. July 31, 2006) (same); *Duqum v. Scottrade, Inc.*, 4:15-CV-1537, 2016 U.S. Dist. LEXIS 89992 (E.D. Mo. July 12, 2016) ("Courts have held that loss of privacy and breach of confidentiality are too abstract to establish Article III standing.")[11]

In sum, the Court finds that plaintiffs lack Article III standing to bring a claim for either damages or injunctive relief because they cannot demonstrate a substantial or certainly impending risk of future identity theft, and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm.[12]

---

[11] The Court also rejects any attempt by plaintiffs to establish standing by alleging that they failed to receive the "benefit of their bargain" by providing their private information to their medical providers, who then entrusted the data to defendants. Other courts that have examined this theory of injury in the context of data breach cases have declined to find that it constitutes an injury-in-fact for Article III standing purposes, and this Court agrees. *See In re Am. Collection Agency Data Sec. Breach Litig.*, 19-MD-2904, 2021 U.S. Dist. LEXIS 240360, *47 (D. N.J. Dec. 16, 2021) (dismissing plaintiffs' claim that they failed to get the "benefit of the bargain" in light of the data breach because even if data security could be considered part of plaintiffs' "bargain" for medical services, plaintiffs did not suffer a particularized injury); *Legg*, 2021 U.S. Dist. LEXIS 232833, *16 (rejecting plaintiff's claim that he suffered concrete injury when he lost the "benefit of the bargain" in providing his personal information because there were no indications that plaintiff paid a premium in exchange for data security or that the data breach diminished the value of services he received); *Remijas v. Neiman Marcus Group*, 794 F.3d 688, 695 (7th Cir. 2015) (describing plaintiff's diminution in value and benefit of the bargain theories as "dubious" and refraining from relying on these theories to support standing).

[12] Because the Court is recommending dismissal for lack of standing, a threshold issue that implicates the Court's subject matter jurisdiction, the Court does not address defendants' other arguments, pursuant to Rule 12(b)(6), that plaintiffs fail to state a claim, on which relief may be granted, for negligence or breach of contract.

CONCLUSION

For the foregoing reasons, the Court recommends granting defendants' motion to dismiss (Dkt. No. 23) and dismissing the consolidated class action complaint for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1).

Pursuant to 28 U.S.C. §636(b)(1), it is hereby **ORDERED** that this Report and Recommendation be filed with the Clerk of Court.

Unless otherwise ordered by Judge Sinatra, any objections to this Report and Recommendation must be filed with the Clerk of Court within fourteen days of service of this Report and Recommendation in accordance with the above statute, Rules 72(b), 6(a), and 6(d) of the Federal Rules of Civil Procedure, and W.D.N.Y. L. R. Civ. P. 72. Any requests for an extension of this deadline must be made to Judge Sinatra.

Failure to file objections, or to request an extension of time to file objections, within fourteen days of service of this Report and Recommendation WAIVES THE RIGHT TO APPEAL THE DISTRICT COURT'S ORDER. *See Small v. Sec'y of Health & Human Servs.*, 892 F.2d 15 (2d Cir. 1989).

The District Court will ordinarily refuse to consider *de novo* arguments, case law and/or evidentiary material which could have been, but were not, presented to the Magistrate Judge in the first instance. *See* Paterson–Leitch Co. v. Mass. Mun. Wholesale Elec. Co., 840 F.2d 985, 990-91 (1st Cir. 1988).

Finally, the parties are reminded that, pursuant to W.D.N.Y. L.R.Civ.P. 72(b), written objections "shall specifically identify the portions of the proposed findings and recommendations to which objection is made and the basis for each objection, and shall

be supported by legal authority." ***Failure to comply with these provisions may result in the District Court's refusal to consider the objection.***

SO ORDERED.

DATED: February 1, 2022
Buffalo, New York

HONORABLE MICHAEL J. ROEMER
United States Magistrate Judge